MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Dipartimento per le Politiche Sociali, del Terzo Settore e Migratorie
DIREZIONE GENERALE DELL'IMMIGRAZIONE E DELLE POLITICHE DI INTEGRAZIONE

Allegato B

MISURE TECNICHE E ORGANIZZATIVE DEL TITOLARE DEL TRATTAMENTO DEI DATI

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Security Policy e procedure per la protezione dei dati personali	A.1	L'organizzazione documenta la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni.
Security Policy e procedure per la protezione dei dati personali	A.2	La politica di sicurezza è riesaminata e aggiornata, se necessario,su base annuale.
Security Policy e procedure per la **protezione dei** dati personali	A.3	L'organizzazione documenta una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica è approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
Security Policy e procedure per la protezione dei dati personali	A.4	La politica di sicurezza fa riferimento a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili del trattamento dei datio per le altre terze parti coinvolte nel trattamento dei dati personali.
Security Policy e procedure per la protezione dei dati personali	A.5	E' creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza.
Ruoli e responsabilità	B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con la politica di sicurezza.
Ruoli e responsabilità	B.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, sono chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
Ruoli e responsabilità	B.3	È effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Policy per il controllo degli accessi	C.1	I diritti specifici di controllo dell'accesso sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
Policy per il controllo degli accessi	C.2	Una politica di controllo degli accessi è dettagliata e documentata. L'organizzazione determina in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nel contesto dei processi e delle procedure relative ai dati personali.
Policy per il controllo degli accessi	C.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, gestione degli accessi) è chiaramente definita e documentata.
Gestione degli asset/risorse	D.1	L'organizzazione dispone di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro include almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica è assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
Gestione degli asset/risorse	D.2	Le risorse IT sono riesaminate e aggiornate regolarmente.
Gestione degli asset/risorse	D.3	I ruoli che hanno accesso a determinate risorse sono definiti e documentati.
Gestione del cambiamento	E.1	L'organizzazione si assicura che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, responsabile IT o sicurezza). Questo processo è monitorato regolarmente.
Gestione del cambiamento	E.2	Lo sviluppo del software è eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire I test, sono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Gestione del cambiamento	E.3	È presente una politica dettagliata e documentata di gestione dei cambiamenti. Include: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di gestione dei cambiamenti è regolarmente aggiornata.
Gestione degli incidenti / Data Breaches	G.1	È definito un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.
Gestione degli incidenti / Data Breaches	G.2	Le violazioni dei dati personali sono segnalate immediatamente alla Direzione. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
Gestione degli incidenti / Data Breaches	G.3	Il piano di risposta degli incidenti è documentato, compreso un elenco di possibili azioni di mìtigazìone e una chiara assegnazione dei ruoli.
Riservatezza del personale	I.1	L'organizzazione garantisce che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di pre-assunzione e / o inserimento.
Riservatezza del personale	I.2	Prima di assumere i propri compiti, il personale è invitato a riesaminare e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	J.1	L'organizzazione garantisce che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali è inoltre adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione.
Formazione	J.2	L'organizzazione dispone di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.
Controllo degli accessi ed autenticazione	K.1	È attuato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema consente la creazione, l'approvazione, il riesame e l'eliminazione degli account degli utenti.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Controllo degli accessied autenticazione	K.2	L'uso di account generici (non personali) è vietato. Nei casi in cui ciò è necessario, si garantisce che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
Controllo degli accessied autenticazione	K.3	È presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo è utilizzata una combinazione di user- id e password. Le password rispettano un certo livello (configurabile) di complessità.
Controllo degli accessied autenticazione	K.4	Il sistema di controllo degli accessi è in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
Controllo degli accessied autenticazione	K.5	Una politica specifica per la password è definita e documentata. La politica include almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.
Controllo degli accessied autenticazione	K.6	Le password degli utenti sono archiviate in formato "hash" con algoritmi crittografici SSNA-256
Logging e monitoraggio	L.1	I log sono attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
Logging e monitoraggio	L.2	I log sono registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzatì. Gli orologi sono sincronizzati con un'unica fonte temporale di riferimento.
Logging e monitoraggio	L.3	Vengono registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modiùca dei diritti di accesso degli utenti.
Logging e monitoraggio	L.4	Non c'è alcuna possibilità di cancellazione o modifica del contenuto dei log. Anche l'accesso ai log è registrato oltre al monitoraggio per rilevare attività insolite.
Logging e monitoraggio	L.5	Un sistema di monitoraggio elabora i log e produce rapporti sullo stato del sistema e notificare potenziali allarmi.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Sicurezza desktop/laptop/mobile	N.1	Gli utenti non sono in grado di disattivare o aggirare le impostazioni di sicurezza.
Sicurezza desktop/laptop/mobile	N.2	Le applicazioni anti-virus e le relative signatures sono configurate su base settimanale.
Sicurezza desktop/laptop/mobile	N.4	Il sistema ha timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
Sicurezza desktop/laptop/mobile	N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema sono installati regolarmente.
Sicurezza desktop/laptop/mobile	N.6	Le applicazioni antivirus e le signature sono configurate su base giornaliera.
Network/Communication security	0.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).
Network/Communication security	0.2	L'accesso wireless al sistema IT è consentito solo a utenti e processi specifici. E' protetto da meccanismi di crittografia.
Network/Communication security	O.3	In generale, l'accesso remoto al sistema IT è evitato. Nei casi in cui ciò sia assolutamente necessario, è eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
Network/Communicatìon security	O.4	Il traffico da e verso il sistema IT è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
Dispositivi portatili/Mobile	Q.1	Le procedure di gestione dei dispositivi mobili e portatili sono definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
Dispositivi portatili/Mobile	Q.3	I dispositivi mobili sono soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali.
Dispositivi portatili/Mobile	Q.4	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili sono chiaramente definiti.
Dispositivi portatili/Mobile	Q.5	L'organizzazione è in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Dispositivi portatili/Mobile	Q.7	I dispositivi mobili sono fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita del software	R.1	Durante il ciclo di vita dello sviluppo si seguono le migliori pratiche, lo stato dell'arte e pratiche, framework o standard di sicurezza ben noti.
Sicurezza del ciclo di vita del software	R.2	Specifici requisiti di sicurezza sono definiti durante le prime fasi del ciclo di vita dello sviluppo.
Sicurezza del ciclo di vita del software	R.3	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET Privacy Enhancer Technologies)) sono adottate in analogia con i requisiti di sicurezza.
Sicurezza del ciclo di vita del software	R.4	Sono seguiti standard e pratiche di codifica sicure.
Sicurezza del ciclo di vita del software	R.5	Durante lo sviluppo, sono eseguiti test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali.
Sicurezza del ciclo di viti del software	R.6	I vulnerability assessment, i penetration test applicativi e dell'infrastruttura sono eseguiti da una terza parte fidata prima del passaggio in ambiente di produzione. Il passaggio non può avvenire a meno che non sia raggiunto il livello di sicurezza richiesto.
Sicurezza del ciclo di vita del software	R.7	Sono eseguiti penetration test periodici.
Sicurezza del ciclo di vita del software	R.8	Si ottengono informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati.
Sicurezza del ciclo di vita del software	R.9	Le patch software sono testate e valutate prima di essere installate in ambiente di produzione.
Sicurezza fisica	T.1	Il perimetro fisico dell'infrastruttura IT non è accessibile da personale non autorizzato.

CATEGORIA	ID	DESCRIZIONE DELLA MISURA
Sicurezza fisica	T.2	L'identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, è stabilita, a seconda dei casi.
Sicurezza fisica	T.3	Le zone sicure sono definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi sono mantenuti e monitorati in modo sicuro
Sicurezza fisica	T.4	I sistemi di rilevamento anti-intrusione sono installati in tutte le zone di sicurezza.
Sicurezza fisica	T.5	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.
Sicurezza fisica	T.7	Un sistema antincendio automatico, un sistema di climatizzazione dedicato e chiuso e un gruppo di continuità (UPS) sono usati nella sala server.
Sicurezza fisica	T.8	Il personale di supporto esterno ha accesso limitato alle aree protette.

Attività e misure specifiche per la CyberSecurity

Sono state effettuate attività di Red Teaming in modalità black box, ovvero senza la condivisione preliminare di informazioni riguardanti l'infrastruttura, le applicazioni o credenziali di accesso ai sistemi. Ciò consente di simulare un attacco da parte di un avversario esterno e di valutare le misure di sicurezza difensive in atto dell'Amministrazione.
La metodologia operativa adottata si basa su un approccio graduale, diviso in fasi ben definite, che permettono di analizzare le vulnerabilità e le debolezze della sicurezza dell'intera Amministrazione.
Di seguito l'elenco delle fasi e delle attività su cui si basa la metodologia:

- Information Gathering / OSINT;
- External Network;
- Social Engineering;
- Internal Network Exploitation.

Infine, nell'ambito dei temi di sicurezza informatica vengono svolte ulteriori attività di Vulnerability Assessment, articolate nelle seguenti fasi:

- Pre-assessment, definita "Security Strategy As Is", con l'obiettivo di finalizzare la definizione di un Security Posture Profile;
- Information Gathering, ovvero raccolta di informazioni sui sistemi informativi in esame;
- Security Architecture As Is Analysis, ovvero analisi della postura di sicurezza dei sistemi informativi in esame;
- Q&A al personale, ovvero conduzione di questionari al personale dell'Amministrazione e valutazione risposte;
- "Security Posture and Security Scoring", finalizzata a condurre attività di analisi delle criticità uomo/macchina attraverso tool, sistemi e framework internazionali e tramite la presa in input dei risultati della prima fase;
- Testing del codice dinamico: Il servizio di testing del codice è orientato all'identificazione delle vulnerabilità software presenti all'interno del codice binario/compilato degli applicativi.